**ODTÜ ENFORMATİK ENSTİTÜSÜ TEZ TANITIM DOKÜMANI**

|  |  |
| --- | --- |
| **Öğrencinin Adı/Soyadı:** | **Özgür Ural** |
| **Kayıtlı olduğu lisansüstü program:** | **Siber Güvenlik** |
| **Tez savunması tarihi:** | **07.08.2010 11.00** |
| **Tez savunması yeri:** | **A – 212 Toplantı Odası** |

**Thesis title:** AUTOMATIC DETECTION OF CYBER SECURITY EVENTS FROM TURKISH TWITTER STREAM AND TURKISH NEWSPAPER DATA

**Tezin başlığı:** TÜRKÇE TWİTTER AKIŞI VE TÜRKÇE GAZETE VERİLERİNDEN SİBER GÜVENLİK OLAYLARININ OTOMATİK TESPİT EDİLMESİ

**Synopsis**:

The present thesis investigates the automatic detection of security incidents in Turkish by processing Twitter and news media. It proposes an automatic, Turkish specific software system that can detect cybersecurity events in real time.

**Sinopsis**:

Bu tez, Twitter ve haber medya kaynaklarındaki Türkçe metinleri işleyerek güvenlik olaylarının otomatik olarak tespit edilmesini araştırmaktadır. Siber güvenlik olaylarını gerçek zamanlı olarak tespit edebilen otomatik, Türk diline özgü bir yazılım sistemi önermektedir.

**Abstract:**

Cybersecurity experts scan the internet and face security events that influence users, institutions, and governments. An information security analyst regularly examines sources to stay up to date on security events in her/his domain of expertise. This may lead to a heavy workload for the information analysts if they do not have proper tools for security event investigation. For example, an information analyst may want to stay aware of cybersecurity events, such as a DDoS (Distributed Denial of Service) attack on a government agency website. The earlier they detect and understand the threats, the longer time remaining to alleviate the obstacle and to investigate the event. Therefore, information security analysts need to establish and keep situational awareness active about the security events and their likely effects. However, due to the large volume of information flow, it may be difficult for security analysts and researchers to detect and analyze security events timely. There have been attempts to solve this problem both from an academic perspective and engineering purposes.

A recent challenge in this domain is that the internet community use different languages to share information. For instance, information about security events in Turkey is mostly shared on the internet in Turkish. The present thesis investigates the automatic detection of security incidents in Turkish by processing Twitter and news media. It proposes an automatic, Turkish specific software system that can detect cybersecurity events in real time.

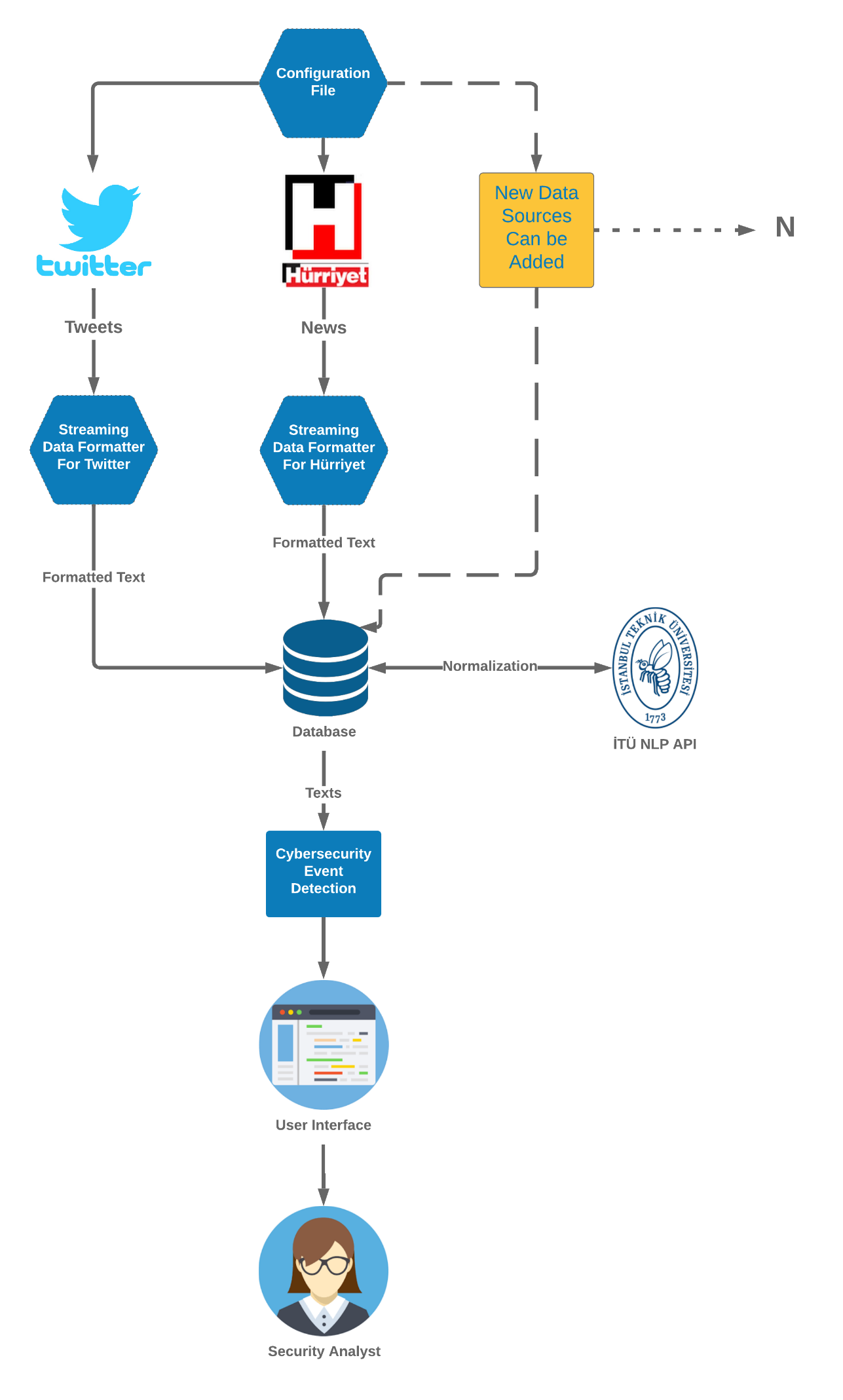
Keywords: Cyber Security, Event Detection, Turkish, Twitter, Hurriyet Newspaper.

**Özet:**

Siber güvenlik uzmanları interneti taramakta ve kullanıcıları, kurumları ve hükümetleri etkileyen güvenlik olaylarıyla karşı karşıya kalmaktalar. Bir bilgi güvenliği analisti, kendi uzmanlık alanındaki güvenlik olaylarından haberdar olmak için kaynakları düzenli olarak inceler. Bu incelemeler, güvenlik olay incelemesi için uygun araçları yoksa, bilgi analistleri için ağır bir iş yüküne yol açabilir. Örneğin, bir bilgi analisti, bir devlet kurumu web sitesine yapılan DDoS (Dağıtılmış Hizmet Reddi) saldırısı gibi siber güvenlik olaylarından haberdar kalmak isteyebilir. Tehditleri ne kadar erken saptar ve anlarsa, engeli azaltmak ve gerçekleşen olayı araştırmak için o kadar uzun süresi kalır. Bu nedenle, bilgi güvenliği analistlerinin, güvenlik olayları ve muhtemel etkileri hakkında durumsal farkındalıklarını oluşturmaları ve aktif tutmaları gerekir. Bununla birlikte, büyük miktarda bilgi akışı nedeniyle, güvenlik analistlerinin ve araştırmacıların güvenlik olaylarını zamanında tespit etmesi ve analiz etmesi zor olabilir. Bu sorunu hem akademik açıdan hem de mühendislik odaklı çözme girişimleri bulunmaktadır.

Bu alandaki son zorluk, internet camiasının bilgi paylaşmak için farklı diller kullanmasıdır. Örneğin, Türkiye ile ilgisi bulunan güvenlik olaylarına ait bilgiler internette çoğunlukla Türkçe olarak paylaşılmaktadır. Bu tez, Twitter ve haber medya kaynaklarındaki Türkçe metinleri işleyerek güvenlik olaylarının otomatik olarak tespit edilmesini araştırmaktadır. Siber güvenlik olaylarını gerçek zamanlı olarak tespit edebilen otomatik, Türk diline özgü bir yazılım sistemi önermektedir.

Anahtar Sözcükler: Siber Güvenlik, Olay Tespiti, Türkçe, Twitter, Hürriyet Gazetesi.



**İmge:** [Tezi temsil eden bir adet imge (grafik, resim, figür, fotoğraf) Word dosyasının içine eklenecektir. İmge PNG formatında, en az 180x180 pixel boyunda, 70 ppi çözünürlükte olacaktır. En/boy oranı 1:1 ve 4:3 arasında olacak.]

**Örnek imge en/boy oranları:**

4:3

1:1

**ÖNEMLİ NOT:** Bu dokümanın içeriği Enformatik Enstitüsü web sayfasındaki tez duyurusunda kullanılacaktır. Tamamlandıktan sonra elektronik kopya olarak bölüm sekreterine iletilmesi gerekmektedir.